Security Quickie 10-4-02: SANS/FBI Top 20 List

SANS, the FBI, other agencies, and individuals have updated the Top 20 Most Critical Internet Security Vulnerabilities List for information systems. A great deal of effort has gone into this revision, and it includes up-to-date information, explanations, and links to patches and fixes. Also included on the SANS/FBI Top 20 website are links to Top 20 testing tools, case studies, and other related issues. This is a great resource for information system administrators, security personnel, auditors, and others. The SANS/FBI Top 20 List can be found at: http://www.sans.org/top20/

Why should the everyday user care?

While most of these top 20 vulnerabilities (10 for Windows, 10 for Unix based) are directed toward systems and security administrators, one critical vulnerability found in each involves every user of every system: weak or non-existent **passwords**.

To quote from sections W7.1 and U10.1 of the Top 20 List:
"Passwords, pass-phrases and security codes are used in virtually every interaction between users and information systems. Most forms of user authentication, as well as file and data protection, rely on user-supplied passwords… a compromised password is an opportunity to explore a system from the inside virtually undetected. An attacker would have complete access to any resources available to that user, and would be significantly closer to being able to access other accounts, nearby machines, and perhaps even administrative privileges. Despite this threat, accounts with bad or empty passwords remain extremely common, and organizations with good password policy far too rare."

Essentially what this means is that the password behavior of not only system administrators but also everyday users should be considered a "Critical Vulnerability". So, as the ITD Operating Security Policy directs (section 12), use good passwords and protect them.
http://das.ite.iowa.gov/security/pdf/itdpolicy.pdf
Every IT user's awareness and behavior is important. By doing using good passwords and protecting them, we are protecting our State, our agency, and ourselves.

For those interested, the list of top vulnerabilities for both Windows and Unix-based systems follows:

Top Vulnerabilities to Windows Systems

- W1 Internet Information Services (IIS)
- W2 Microsoft Data Access Components (MDAC) -- Remote Data Services
- W3 Microsoft SQL Server
- W4 NETBIOS -- Unprotected Windows Networking Shares
- W5 Anonymous Logon -- Null Sessions
- W6 LAN Manager Authentication -- Weak LM Hashing
- W7 General Windows Authentication – Account with No Passwords or Weak Passwords
- W8 Internet Explorer
- W9 Remote Registry Access
- W10 Windows Scripting Host

Top Vulnerabilities to Unix Systems

- U1 Remote Procedure Calls (RPC)
- U2 Apache Web Server
- U3 Secure Shell (SSH)
- U4 Simple Network Management Protocol (SNMP)
- U5 File Transfer Protocol (FTP)
- U6 R-Services -- Trust Relationships
- U7 Line Printer Daemon (LPD)
- U8 Sendmail
- U9 BIND/DNS
- U10 General Unix Authentication -- Accounts with No Passwords or Weak Passwords